

CLAIMS

- 1 1. A data authentication system comprising:
 - 2 A. an integrity check processor that
 - 3 i. selects one or more integrity functions from a set of functions, and
 - 4 ii. manipulates m selected data bytes from each of one or more data
 - 5 packets in accordance with the selected integrity check functions to
 - 6 produce one or more integrity checks that correspond to the one or
 - 7 more data packets; and
 - 8 B. an integrity block processor that encrypts the one or more integrity checks
 - 9 produced by the integrity check processor and produces an integrity block that is
 - 10 used to authenticate the data packets.
- 1 2. The data authentication system of claim 1 wherein the integrity check processor in-
2 cludes in the integrity check an indication of which integrity function to select.
- 1 3. The data authentication system of claim 2 wherein the indication is a function identi-
2 fier.
- 1 4. The data authentication system of claim 2 wherein the indication is an offset value for
2 a pseudorandom sequence known to a sender and an intended recipient.
- 1 5. The data authentication system of claim 4 wherein the pseudorandom sequence is
2 generated using a seed value known by the sender and the intended recipient.
- 1 6. The data authentication system of claim 1 wherein the integrity check processor uses
2 information in the one or more data packets as one or more offset values for a pseudoran-
3 dom sequence known to a sender and an intended recipient.
- 1 7. The data authentication system of claim 6 wherein the pseudorandom sequence is
2 generated using a seed value known by the sender and the intended recipient.

1 8. The data authentication processor of claim 2 wherein the integrity check processor
2 selects more than one integrity function for a given data packet and includes in the integ-
3 rity check information that identifies a list of the selected functions and a corresponding
4 list of the results of the manipulations.

1 9. The data authentication system of claim 1 wherein the integrity block processor en-
2 crypts the integrity checks in accordance with a secret key that is shared by intended re-
3 cipients of the data packets.

1 10. The data authentication system of claim 1 wherein the integrity check processor se-
2 lects the m data bytes at random from a first data packet, and for any remaining data
3 packets selects data bytes that are offset from the data bytes selected from the first data
4 packet.

1 11. The data authentication system of claim 1 wherein the integrity block processor en-
2 crypts into the integrity block information that identifies the data bytes selected from
3 each of the data packets.

1 12. The data authentication system of claim 11 wherein the information includes data
2 byte interval and offset values.

1 13. The data authentication system of claim 1 wherein the integrity check processor in-
2 cludes in the integrity checks one or more sequence numbers that are associated with the
3 data packets.

1 14. The data authentication system of claim 1 wherein the integrity block processor as-
2 sembles the plurality of integrity checks in an order that differs from the order of the data
3 packets and encrypts into the integrity block information that associates the integrity
4 checks with the appropriate data packets.

1 15. The data authentication system of claim 14 wherein the integrity block processor en-
2 crypts into the integrity block a list of sequence numbers that corresponds to the order of
3 the integrity checks within the integrity block.

1 16. The data authentication system of claim 1 wherein the integrity check processor pro-
2 duces digital signatures for one or more of the data packets and includes the digital sig-
3 natures in the respective data packets.

1 17. The data authentication system of claim 1 wherein the integrity block processor pro-
2 duces a digital signature for the integrity block and includes the digital signature in the
3 integrity block.

1 18. The data authentication system of claim 1 wherein the selected integrity check func-
2 tion concatenates the selected data bytes from a given data packet to produce the associ-
3 ated integrity check.

1 19. The data authentication system of claim 1 further including a chaff processor for pro-
2 ducing for transmission extraneous packets that are associated with and do not pass one
3 or more of the integrity checks, the chaff processor including the extraneous packets in a
4 transmission that includes the data packets.

1 20. The data authentication system of claim 1 wherein the integrity block processor en-
2 crypts into the integrity block executable code that performs the selected integrity check
3 function.

1 21. The data authentication system of claim 20 wherein the integrity block processor
2 signs the executable code with a digital signature.

1 22. A communications network comprising:

2 A. one or more sending stations for sending data packets;

- 3 B. one or more recipient stations for receiving the data packets sent by the
4 sending stations; and
- 5 C. an authentication system that includes
- 6 i. an integrity block processor
- 7 a. for selecting one or more integrity functions from a set of
8 integrity functions,
- 9 b. manipulating one or more selected data bytes from a given
10 data packet in accordance with the one or more selected
11 integrity check functions to produce the corresponding in-
12 tegrity check, and
- 13 c. encrypting the one or more integrity checks that are associ-
14 ated with one or more data packets to produce an integrity
15 block and including the integrity block in a transmission to
16 the recipient stations, and
- 17 ii. authentication means for decrypting a received integrity block to
18 reproduce the one or more integrity checks and using information
19 contained in the reproduced integrity checks to select one or more
20 integrity check functions and one or more data bytes to use to de-
21 termine if data in the associated one or more data packets have
22 been altered.

1 23. The communications network of claim 22 wherein the authentication means selects
2 the one or more integrity check functions for use in authenticating the data packets based
3 on identifying information in the associated integrity check.

1 24. The communications network of claim 22 wherein the authentication means uses in-
2 formation in the integrity check or in the associated data packet as an offset value into a
3 pseudo random sequence known to the sender and an intended recipient and uses the next
4 n bits of the sequence to identify the selected integrity check.

1 25. The communications network of claim 22 wherein the authentication means uses the
2 one or more integrity checks, the integrity check functions identified therein and the se-
3 lected data bytes from the one or more data packets to determine if the data packets have
4 been altered.

1 26. The communications network of claim 22 wherein the integrity block processor is
2 included in each of the one or more sending stations and the authentication means is in-
3 cluded in each of the one or more recipient stations.

1 27. The communications network of claim 22 wherein the integrity block processor en-
2 crypts the integrity checks and the authentication means decrypts the integrity blocks in
3 accordance with one or more secret keys that are shared by the sending stations and the
4 intended recipient stations.

1 28. The communications network of claim 22 wherein the integrity block processor se-
2 lects one or more data bytes at random from a first data packet and selects from the re-
3 maining data packets data bytes that are offset from the data bytes selected from the first
4 data packet based on the information contained in the associated integrity checks.

1 29. The communications network of claim 22 wherein the integrity block processor en-
2 crypts into an integrity block the information that identifies the integrity check function.

1 30. The communications network of claim 22 wherein the integrity block processor en-
2 crypts into an integrity block the information that identifies the data bytes selected for
3 each of the one or more data packets by the integrity block processor.

1 31. The communications network of claim 30 wherein the information includes data byte
2 interval and offset values.

1 32. The communications network of claim 22 wherein the integrity block processor fur-
2 ther includes in the integrity block sequence numbers that correspond to the associated
3 data packets.

1 33. The communications network of claim 22 wherein the authentication means assem-
2 bles the integrity checks in an order that differs from the order of the associated data
3 packets and encrypts into the integrity block information that associates the integrity
4 checks with the appropriate data packets.

1 34. The communications network of claim 33 wherein the authentication means further
2 encrypts into the integrity block a list of data packet sequence numbers that corresponds
3 to the order of the integrity checks within the integrity block.

1 35. The communications system of claim 22 wherein the authentication means further
2 produces a digital signature for each data packet and includes the digital signature in the
3 data packet.

1 36. The communications system of claim 22 wherein the authentication means concate-
2 nates selected data bytes from a given data packet to produce the associated integrity
3 check.

1 37. The communications system of claim 22 wherein the authentication means encodes
2 selected bytes from a given data packet to produce the associated integrity check.

1 38. The communications system of claim 22 further including a chaff processor that pro-
2 duces for transmission one or more extraneous packets that are associated with and do not
3 pass one or more of the integrity checks, the chaff processor including the extraneous
4 packets in a transmission with the associated data packets.

1 39. The communications system of claim 22 wherein the integrity block processor further
2 includes in the integrity block executable code that performs an integrity check process.

1 40. The communications system of claim 39 wherein the integrity block processor in-
2 cludes in an integrity block a digital signature that corresponds to the executable code.

1 41. A method of authenticating data that is sent in data packets, the method including the
2 steps of:

- 3 A. selecting one or more integrity functions from a set of integrity functions;
- 4 B. manipulating selected data bytes from a first data packet in accordance
5 with one or more of the selected integrity functions to produce an integrity
6 check;
- 7 C. encrypting the integrity check to produce an integrity block;
- 8 D. sending the integrity block to intended recipients.

1 42. The method of claim 41 further including the steps of:

- 1 E. decrypting a received integrity block to reproduce the integrity check;
- 2 F. selecting one or more integrity check functions from the set of functions;
- 3 G. using the reproduced integrity check and the selected integrity check
4 functions to determine if the first data packet is authentic.

1 43. The method of claim 42 further including the steps of

- 2 H. manipulating data bytes from additional data packets in accordance with
3 one or more of the selected integrity check functions to produce additional
4 integrity checks;
- 5 I. encrypting the additional integrity checks into the integrity block;
- 6 J. decrypting the received integrity block to reproduce the additional integ-
7 rity checks;
- 8 K. selecting one or more integrity check functions; and
- 9 L. using the reproduced additional integrity checks and the selected integrity
10 check functions to determine if respective additional data packets are
11 authentic.

1 44. The method of claim 41 wherein the step of selecting the integrity functions includes
2 providing associated identifiers as part of the integrity check.

1 45. The method of claim 41 wherein the step of selecting the integrity functions includes
2 i. using information in the data packet as an offset value into a pseudorandom
3 sequence, and
4 ii. using the next n bits of the sequence as the integrity function identifier.

1 46. The method of claim 43 further including in the step of encrypting the integrity
2 checks, performing the encryption in accordance with a secret key that is available to the
3 recipients.

1 47. The method of claim 46 further including in the step of decrypting the integrity
2 block, decrypting the block in accordance with the secret key.

1 48. The method of claim 43 wherein the step of manipulating data bytes selects the data
2 bytes at random from the first data packet and selects from the additional data packets
3 data bytes that are offset from the data bytes selected from the first data packet.

1 49. The method of claim 43 wherein the step of encrypting the integrity checks further
2 includes encrypting into the integrity block information that identifies the data bytes se-
3 lected from the data packets.

1 50. The method of claim 43 further including in the step of encrypting the integrity
2 checks the step of encrypting into the integrity block data byte interval and offset values.

1 51. The method of claim 43 wherein the step of manipulating the data bytes to produce
2 the integrity checks further includes the step of including in the integrity checks sequence
3 numbers that correspond to the associated data packets.

1 52. The method of claim 43 wherein the step of encrypting the integrity checks includes
2 assembling the integrity checks in an order that differs from the order of the associated
3 data packets.

4 53. The method of claim 52 wherein the encrypting step further includes the step of en-
5 crypting into the integrity block a list of sequence numbers that corresponds to the order
6 of the integrity checks.

1 54. The method of claim 43 further including the step of producing a digital signature for
2 each data packet and including the digital signature in the data packet.

1 55. The method of claim 42 further including the step of producing a digital signature for
2 the integrity block and including the signature in the block.

1 56. The method of claim 43 wherein the step of manipulating the selective data bytes
2 includes concatenating the selected data bytes from a given data packet to produce the
3 associated integrity check.

1 57. The method of claim 43 wherein the step of manipulating the selected data bytes in-
2 cludes encoding the selected bytes from a given data packet to produce the associated in-
3 tegrity check.

1 58. The method of claim 42 further including the step of including in a transmission ex-
2 traneous packets that are associated with and do not pass one or more of the integrity
3 checks.

1 59. The method of claim 42 wherein the step of encrypting the integrity checks further
2 includes encrypting into the integrity block executable code that performs an integrity
3 check process.

1 60. The method of claim 59 wherein the encrypting step further includes encrypting into
2 the integrity block a digital signature associated with the code.

1 61. A data authentication system comprising:

2 A. an integrity block processor that receives a plurality of data packets and an
3 associated integrity block, the integrity block processor manipulating the integrity
4 block to produce a plurality of integrity checks that correspond to the data pack-
5 ets, and

6 B. an integrity check processor that uses the integrity checks, integrity check
7 functions selected from a set of functions and selected data bytes from the data
8 packets to determine if any of the data packets have been altered.

1 62. The authentication system of claim 61 wherein the integrity block processor further
2 produces from the integrity block information to determine which data bytes to select
3 from the data packets.

1 63. The authentication system of claim 61 wherein the integrity block processor pro-
2 duces from the integrity block information to select which integrity check functions to
3 use to manipulate the selected data packets.

1 64. The authentication system of claim 63 wherein the information determines which
2 function or functions to use for each data packet.

1 65. The authentication system of claim 61 wherein the integrity block processor decrypts
2 the integrity block to produce the plurality of integrity checks.

1 66. The authentication system of claim 65 wherein the integrity block processor uses a
2 shared secret key to decrypt the integrity block.

1 67. The authentication system of claim 65 wherein the integrity block processor decrypts
2 the integrity block to provide to the integrity check processor executable code to use to
3 manipulate the selected data bytes.

1 68. The authentication system of claim 62 wherein the integrity block processor decrypts
2 the integrity block to produce the integrity checks and the integrity check processor uses
3 information in the integrity checks to determine which data bytes to select from the one
4 or more data packets.

1 69. The authentication system of claim 63 wherein the integrity check processor uses a
2 digital signature included in the integrity block to authenticate the integrity block.

1 70. The authentication system of claim 61 wherein the integrity check processor uses one
2 or more digital signatures included in the one or more data packets to further authenticate
3 the data packets.

1 71. A system for authenticating one or more data packets, the system comprising:

2 A. means for configuring at least one sending station with an authentication proc-
3 ess adapted to produce an encrypted integrity block from one or more integrity checks
4 associated with one or more data packets and one or more integrity functions selected
5 from a set of integrity functions;

6 B. means for configuring at least one receiving station with an authentication
7 process adapted to decrypt a received integrity block into one or more integrity checks
8 and authenticate the associated one or more data packets using the one or more integrity
9 checks and associated selected integrity functions.

1 72. The system of claim 71 wherein the receiving station selects, based on information
2 contained in the integrity block, the one or more integrity functions from the set of func-
3 tions and one or more selected data bytes from each of the one or more packets to use in
4 the authentication process.

1 73. The system of claim 71 wherein the means for configuring at least one sending sta-
2 tion includes a computer readable medium containing executable program instructions.

1 74. The system of claim 71 wherein the means for configuring at least one receiving sta-
2 tion includes a computer readable medium containing executable code.

1 75. The system of claim 71 further including means for configuring the sending station
2 to transmit extraneous data packets that are associated with the integrity block but do not
3 pass authentication.

1 76. A computer data signal embodied in a carrier wave and representing sequences of
2 instructions for authenticating data packets, the instructions comprising instructions for:
3 configuring at least one sending station to produce an encrypted integrity block
4 for a plurality of data packets using one or more integrity check functions selected from a
5 set of integrity check functions; and
6 at the configured sending station selecting one or more data bytes from each data
7 packet and producing an associated integrity check that is used with the integrity checks
8 for the other data packets to produce the encrypted integrity block.

1 77. The computer data signal of claim 76 wherein the selection of data bytes from a first
2 data packet is random and the data bytes selected from remaining data packets are offset
3 from the data bytes selected from first data packet.

1 78. The computer data signal of claim 76 wherein the integrity block is encrypted in ac-
2 cordance with a shared secret key.

1 79. The computer data signal of claim 76 wherein the one or more integrity checks are
2 produced by concatenating selected data bytes from respective data packets.

1 80. The computer data signal of claim 76 wherein the one or more integrity checks are
2 produced by encoding selected data bytes from respective data packets.

83. The computer data signal of claim 76 further including configuring the sending station to transmit one or more extraneous data packets that are associated with the integrity block but do not pass authentication tests.

